ARCTIC WOLF

THE LEADER IN SECURITY OPERATIONS

CYBER RISK MANAGEMENT BUYER'S GUIDE

How to Select a Solution for Your Organization

TABLE OF CONTENTS

01 EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

There's a disparity between the growing budget businesses dedicate to cybersecurity and their ability to defend an expanding attack surface. Every year, organizations pour more money into protecting themselves from cyber threats, yet they continue to face tremendous risks.

The size of the information security and risk management technology market is $150.4 billion, according to a 2021 estimate by Gartner.[1] Even so, Verizon's most recent Data Breach Investigations Report tallied 5,258 confirmed data breaches between November 2020 and October 2021.[2] That's up 33% from the 12 months prior.[3]

Why is cybersecurity so ineffective?

The short answer is that cybersecurity tools aren't the problem. It's lack of expertise, alert fatigue, and security infrastructure complexity that cause operational failures. Until you can solve those challenges, you'll continue to struggle with blind spots and leave yourself vulnerable.

For organizations that can't maintain effective security operations because they lack the necessary resources, managed cyber risk brings many advantages.

We created this guide to help you understand the benefits of managed cyber risk, as well as what criteria to consider when evaluating solutions.

Cybersecurity tools aren't the problem. ***It's a lack of expertise, alert fatigue, and security infrastructure complexity that causes operational failures.***

02

UNDERSTANDING DIGITAL RISK

UNDERSTANDING DIGITAL RISK

The growing attack surface compounds cyber risks for organizations. The implementation of new digital initiatives, the adoption of the Internet of Things (IoT), and the continued move to the cloud help drive innovation, but at the cost of an increased exposure to threats.

Effective security operations start with understanding your digital risks. But keep in mind that the reality for overwhelmed security teams is that, even with the best technology and processes in place, it's impossible to address all risks — something somewhere will always need patching.

That's where risk-based vulnerability management comes in. It's a proactive strategy that reduces your attack surface and improves your security posture by helping you focus on your most critical risks. In 2022, according to Gartner, "organizations that use the risk-based vulnerability management method will suffer 80% fewer breaches."[4]

To manage digital risk well, you need to look at the whole picture across your IT landscape: from endpoints and network to your cloud infrastructure.

Some of the commonly overlooked risks include:

System Misconfigurations:

Traditional vulnerability assessments focus on scanning for software defects but miss other critical risks such as system misconfigurations on endpoints. Examples include unnecessarily open ports, inactivated security features, default passwords, and unpatched hardware.

Cloud Infrastructure Misconfigurations:

As the 2021 SocialArks data breach demonstrated, a misconfigured cloud database can wreak major havoc. And these types of cloud security issues are common—Arctic Wolf data shows that nearly half of detected security incidents include a cloud component.[5]

Account Takeover:

More than 80% of hacking-related breaches involve brute force or the use of lost or stolen credentials.[6] Every compromised corporate account increases your risk of a data or systems breach, and stolen credentials are abundantly available on the dark web for sale or for lease—sometimes even for free.

03

5 STEPS TO MANAGING YOUR DIGITAL RISK

03

5 STEPS TO MANAGING YOUR DIGITAL RISK

QUICK REFERENCE

5 Steps to Managing Your Digital Risk

01

Get complete visibility into your environment.

Important to know:

You can't protect what you can't see. But many organizations don't have (or can't monitor) an accurate inventory of assets across endpoints, networks, and cloud environments.

02

Assess your vulnerabilities and prioritize risks.

Important to know:

Simply knowing your vulnerabilities is not enough to effectively mitigate risks. You need to prioritize mitigation of those that may have the greatest business impact and cause the most damage.

03

Detect, monitor, and respond to threats 24x7.

Important to know:

Bad actors don't keep office hours – in fact, 35% of all threats come in after hours. Without human experts monitoring your environment around the clock, you can't respond to threats immediately and minimize the window of opportunity for an attack.

04

Include people, processes, and technology in your strategy.

Important to know:

Your technology stack is only part of your security strategy. Your people and processes play just as big a role.

05

Align security operations with your business goals.

Important to know:

To improve your security posture over time, your security team must follow the processes and workflows that will bring the desired outcomes.

04 THE ADVANTAGES OF A MANAGED RISK SOLUTION

THE ADVANTAGES OF A MANAGED CYBER RISK SOLUTION

A managed risk solution brings a variety of benefits, and helps you:

Identify security vulnerabilities in your endpoints, networks, and cloud infrastructure, as well as user behavior.

Prioritize risks so you can focus on mitigating the ones that have the greatest business impact.

Create actionable reports to mitigate risks, along with strategic guidance to continuously improve your security program.

Improve the effectiveness of your security operations by combining vendor-neutral technology with cybersecurity experts who can monitor your environment 24x7.

Note that risk management is different from managed detection and response (MDR), which monitors and responds to threats in your environment. Risk management enables you to proactively eliminate risks and reduce your exposure.

What's more, unlike endpoint solutions that only give you visibility into your hosts, risk management provides a complete view of your cloud and network infrastructure.

Closing the Vulnerability Window

The rate of vulnerabilities continues to increase each. 2021 broke records, with over 20,000 vulnerabilities identified— a 10% increase from 2020. And it's not just the number of vulnerabilities that's increasing, so too is the damage they can do.

Consider the 2021 T Mobile data breach that compromised the data of over 50 million people. The attacker, an American expat living in Turkey, was able to gain access through an unprotected router and a flaw in the company's internet addresses.

The simple fact is this: You can't protect what you don't know. Because T Mobile didn't have full visibility of their attack surface, they didn't know the vulnerability even existed, let alone have a plan to remediate it. And it's just one of many examples of a breach that could have easily been avoided. Asset discovery and classification is the critical first step in building a robust vulnerability management program.

Attackers act quickly on an opportunity. Managed cyber risk solutions help you get ahead of adversaries by closing gaps in posture and reducing the likelihood of an attack.

05

KEY MANAGED RISK FEATURES AND CAPABILITIES

KEY MANAGED RISK FEATURES & CAPABILITIES

DISCOVER

External Scanning

These vulnerability assessments cover external-facing assets such as firewalls, cloud infrastructure, and web applications. Additionally, some vendors offer cloud security posture management and account takeover risk detection as part of external scanning.

Internal Scanning

Focused on your core IT infrastructure, internal scanning identifies vulnerabilities that result from vectors like misconfigurations and unpatched or outdated apps. Continuous internal scans cover IP-connected devices and endpoints, such as mobile devices, workstations, and IoT devices.

Host-Based Scanning

Using agents that run on devices, host-based scanning monitors active processes, applications, and configurations that violate set policies. It also enables you to take inventory of hardware and software running on the hosts, giving you an inside view of endpoints.

Account Takeover Risk Detection

By continuously scanning the dark and gray web for corporate credentials harvested in data breaches, account takeover detection enables you to quickly take action to secure compromised accounts. Typically, your solution partner provides details such as the source, description of the data breach involved, and the exposed emails.

ASSESS

Security Risk Scoring

For effective risk management, you need to know if your security posture improves or declines over time. Benchmarking against other organizations in similar industries helps you understand where you stand and how to improve.

Asset Inventory

Your attack surface constantly changes as you add more users and hosts. To build and maintain a comprehensive inventory of assets, dynamic asset identification profiles and classifies your IT assets automatically and continuously so that no new asset falls through the cracks.

Asset Criticality

Assigning an asset a level of criticality as an attribute to be used in risk prioritization provides a standardized critical labeling system with a clear definition of importance of the asset. The level of asset criticality can be critical, high, medium, low, or unassigned.

Asset Tagging

Managed risk allows you to gain additional asset context of your risk prioritization efforts. It helps with asset classification and asset organization efforts. You can use asset tags to pivot and review assets as well as your risks during your risk management and hardening efforts. It makes the automation of managing assets possible, makes reports more meaningful for the business, and improves risk prioritization efforts.

HARDEN

Configuration Benchmarking

To help you prioritize your risk mitigation, configuration benchmarking is a risk score based on criteria such as the attack vector accessibility, attack complexity, and the impact of accessed data. These benchmarks provide context so you can address the most critical misconfigurations first.

Risk Remediation Steps

Managed risk allows you to export a report with remediation resources against your risk, vulnerabilities, and assets. By including the remediation steps alongside the vulnerabilities, you can efficiently—and consistently—remediate known risks.

Cloud Security Posture Management (CSPM)

A solution that protects against misconfigurations, mismanagement, and other mistakes occurring in cloud infrastructure, CSPM includes prevention, detection, and response capabilities based on criteria such as security frameworks, IT policies, and regulatory compliance.

06

TOP CRITERIA FOR EVALUATING CYBER RISK MANAGEMENT VENDORS

TOP CRITERIA FOR EVALUATING CYBER RISK MANAGEMENT

287 DAYS

The average time it takes to identify and contain a data breach.

–IBM Security, Cost of a Data Breach Report

When evaluating potential partners, look for:

DISCOVERY

— The ability to discover and gain visibility to your current digital and attack surface.

ASSESS

— An understanding of your cyber risk in the context of your business.

HARDENING

— Expertise to guide your strategy and help you harden your environment.

TOP CRITERIA FOR EVALUATING CYBER RISK MANAGEMENT

Check if the vendor can offer a solution that offers:

CONCIERGE LED MANAGED RISK EXPERIENCE

Strategic Recommendations: Offers advice to help you continuously improve security posture.

24x7 Digital Risk Monitoring: Provides around-the-clock monitoring for vulnerabilities, system misconfigurations, and account takeover risks.

Personalized Engagement: Sets regular meetings with a named security operations expert to review your overall security posture and find areas of improvement that are optimized for your environment.

DISCOVERY

Allows you to identify and gain visibility to your current digital and attack surface.

Attack Surface Coverage:
Covers endpoints, network, and cloud—and goes beyond vulnerability assessments.

Dynamic Asset Discovery:
Offers the automatic and continuous ability to map and profile your assets.

Account Takeover Risk Detection:
Continuously scans the dark and gray web for corporate credentials harvested in data breaches.

ASSESSMENT

Determines your cyber risk in the context of your business.

Classification and contextualization:
Helps you inventory your assets and vulnerabilities, and then provides a risk baseline that gives you a deeper understanding of your attack surface.

Risk Scoring:
Provides a quantified view of all digital risks in your environment, which are weighted based on severity and benchmarked against industry peers. CST asses your current risk posture and identify gaps relative to best practices.

Concierge-Led Prioritization:
Prioritization tailored to your business context, revealing your overall digital risk.

HARDENING

Identifies exposure and adjusts your strategy to help you harden your environment.

Security Controls Benchmarking:
Tracks configuration errors and other controls over time.

Actionable On-demand Reporting:
Creates automated reports with risk assessments, trends, action lists, and other details in an easy-to-consume and shareable format.

Guided Remediation:
Offers expertise that helps you through your remediation process.

Risk Management Plans:
Allows you to creates schedules to prioritize remediation, track progress, and close risks faster.

07

IMPORTANT QUESTIONS TO ASK VENDORS

07

IMPORTANT QUESTIONS TO ASK VENDORS

When evaluating solutions, answers to the following questions will help you make an informed decision.

In 2021 the potential cost of ransomware in the United States was over $20 billion

–CyberCrime Magazine[7]

Processes and Capabilities

- Can you scan endpoints, networks, and cloud environments?
- How do you get visibility into the threats? (e.g., is there an easy-to-understand cloud-based dashboard/platform?)
- How often do you scan?
- How do you prioritize vulnerabilities?
- Can you categorize assets?
- What proactive tactics do you use?
- How do you quantify the risks so I can act?
- Does your solution monitor user-based risks?
- Can you quantify dark-web exposures?
- How do you identify misconfigurations?

Solution Offering

- How do you measure success?
- How does your solution support my compliance needs?
- Will I receive a dedicated point of contact and support?
- How does your solution scale and tailor to my needs?
- Does the solution offer configurable, custom scheduling for scans?

08 FINAL THOUGHTS

FINAL THOUGHTS

With technology-driven growth and innovation, protecting your environment becomes exponentially more challenging. You need a comprehensive view of your digital risks, which goes beyond vulnerabilities.

Resource constraints limit security teams' abilities to proactively close security gaps. Yet this is not a tools problem, it is an operational one.

Adding the latest technology and security products won't solve these challenges. Achieving security outcomes that align with your business goals requires a strategy that includes people, processes, and technology.

Organizations are starting to see the value security operations bring to improving the overall effectiveness of their security programs. Yet implementing an in-house security operations model runs into many of the same problems that make security inefficient in the first place: a lack of expertise and resources.

A managed risk solution solves this challenge by taking some of the day-to-day burden off your in-house team's shoulders. But more importantly, it provides an effective way to protect your network, endpoints, and cloud infrastructure —and includes access to experts who can offer both tactical and strategic insights.

A managed solution can be a critical part of your success. Take the time to evaluate potential vendors to ensure you choose a highly experienced and responsive partner that is well suited to your needs.

Sources
1. Forecast Analysis: Information Security and Risk Management, Worldwide by Shailendra Upadhyay
2. 2021 Verizon Data Breach Investigation Report
3. 2021 Verizon Data Breach Investigation Report
4. "Implement a Risk-Based Approach to Vulnerability Management," Prateek Bhajanka and Craig Lawson, Gartner
5. Arctic Wolf 2021 Data Breaches in Review
6. 2020 Data Breach Investigations Report, Verizon
7. CyberCrime Magazine

ARCTIC WOLF

SOC2 TYPE II CERTIFIED

AICPA SOC

ISO 27001 CERTIFIED CYBERGUARD COMPLIANCE

CONTACT US

arcticwolf.com | 1.888.272.8429 | ask@arcticwolf.com

ARCTIC WOLF

ABOUT ARCTIC WOLF

THE LEADER IN SECURITY OPERATIONS

Arctic Wolf® is a global leader in security operations, delivering the first cloud-native security operations platform designed to end cyber risk. Powered by threat telemetry spanning endpoint, network, and cloud sources, the Arctic Wolf® Security Operations Cloud ingests and analyzes trillions of security events a week across the globe, enabling critical outcomes for most security use cases. The Arctic Wolf® Platform delivers automated threat detection and response at scale and empowers organizations of any size to stand up world-class security operations with the push of a button.

For more information about Arctic Wolf, visit arcticwolf.com.